A summary of New Data Protection Principles in terms of the General Data Protection Regulations (GDPR)

Introduction

The Data Protection Legislation in the UK will change on 25 May 2018 with the adoption of the EU's General Data Protection Regulations (GDPR). The current data protection rules and regulations will be updated with new principles, while other current principles will be adapted or changed.

This is an important development for all organisations that hold personal data since Data Protection Legislation covers everyone about whom the organisation keeps personal data. Such data can belong to employees, volunteers, service users, members, supporters and donors.

Please be aware that the United Kingdom will adopt the GDPR as it is. The UK Government indicated that Brexit will not influence this process at all.

Many of the principles of the GDPR are similar to current data protection legislation. That means that if the organisation is already in compliance with current data protection legislation, many of these principles will already be in compliance with the GDPR. However, as there are a number of new elements and enhancements, organisations will have to start doing setting new things in place and adapt other existing principles.

Every organisation should in any case have a written policy and procedure for dealing with personal data. This policy, about how they handle personal data and enact privacy principles, should be specific to their specific context and the market they function in.

This paper will not deal with the specifics of what a written data protection policy should be, but will rather focus on answering two questions. The first question is: "What is the GDPR?". The second question is: "How would a Not-for-Profit Organisation, such as the South African Congregation (SAC), go about ensuring that it is in compliance with the requirements of the GDPR?"

A very handy tool for organisations looking towards GDPR compliance is the Information Commissioner's Office (ICO) website. The ICO website (www.ico.org.uk) contains a number of very useful links on proceeding with implementing the GDPR.

[1] What is the GDPR?

Simply put, the GDPR is the new legislation that aims to regulate the processing, use and sharing of individuals'' personal data. It updates rights for a networked world. In this regard there are a number of key concepts to be aware of.

The rights and obligations of different parties to the GDPR are determined by whether they are the 'Data Subject', the 'Controller' or the 'Processor' of the data. Furthermore, was there 'Consent' by the 'Data Subject' for the 'Processing' of their 'Personal Data'?

For the purpose of the SAC, its responsibilities in this regard will be conditional on whether it's the Controller or the Processor of their congregation's personal data.

It is important therefore to understand what is meant with each of these key concepts.

Data Subject means the identified or identifiable natural person whose personal data information is the subject of the matter. In SAC's case, this would be a member of the congregation for example.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. SAC is the Controller of personal data they hold for the members of their congregation.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Does SAC process the personal data, or do they make use of another processor who acts on its behalf?

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Personal Data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The GDPR sets in place a data protection model which regulates the rights of the different parties involved in the Data Protection process. The Controllers, Processors and Data Subjects all fall under a Supervisory Authority. This authority, which in the UK is called the Information Commissioner's Office (ICO), assesses the compliance of the Controllers and Processors in terms of the GDPR and also enforces penalties on these parties, where applicable. The ICO is also the body that Data Subjects can complain to if their Data Protection rights were infringed upon by specific Controllers.

The Data Subjects have the right to compensation from the Controller or Processor where they suffered material or non-material damage as a result of data processing. The ICO can also fine organisations that negligently or intentionally infringed upon the rights of the Data Subject.

For SAC this means that it has to ensure that its data protection procedures are robust and sufficient to ensure adequate protection of its data subjects' personal data and to ensure that there is no infringement on the subjects' rights. Otherwise, it can potentially have a financial impact on the organisation.

[2] The GDPR legislation:

- Requires organisations to register with the ICO if they keep records. **Is the SAC registered with the ICO?**
- Governs the processing of personal data including 'personal sensitive data'. Please note, a data subject's religion is one of the categories of personal sensitive data.
- **Requires organisations to comply with eight principles** (https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/), which are:

1. **Personal data shall be processed fairly and lawfully** (https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/) and, in particular, shall not be processed unless –
    a. At least one of the conditions in Schedule 2 *(attached)* is met, and
    b. In the case of sensitive personal data, at least one of the conditions in Schedule 3 *(attached)* is also met.
2. **Personal data shall be obtained only for one or more specific and lawful purposes**, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. **Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed**.
4. **Personal data shall be accurate** and, where necessary, **kept up to date**.
5. **Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose** or those purposes.
6. Personal **data shall be processed in accordance with the rights of data subjects under this Act.**

7. Appropriate technical and organisational **measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data**.
8. Personal data **shall not be transferred to a country or territory outside the European Economic Area** unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

- **Allows employees, service users and other contacts to request to see the personal data held on them**. This is called the **Data Access Request**.

[3] How would the SAC ensure compliance with the GDPR?

The ICO specifically sets out 12 steps (https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf) for organisations to follow in their preparation of GDPR compliance. These steps, which are similar to those set out on the *Knowhow Non Profit* (KNP) website (www.knowhownonprofit.org), form the basis of this section. While the ICO sets out these steps generally, the KNP focusses on the so-called Non Profit sectors.

Step 1: Awareness

Ensure that the **employees** of the organisation, especially those key staff and decision makers that directly deal with data protection, **know about the upcoming changes**. These individuals should be made aware of the impact of the GDPR on their organisation and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at the **organisation's risk register**, if it has one.

Implementing the GDPR could also have significant resource implications, depending on its complexity. Compliance preparations should therefore not be left until the last minute.

Staff should therefore be adequately trained. New employees must receive **data protection training** to explain how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff.

Step 2: Information the organisation holds

The SAC should **document what personal data it holds**, where it came from and who it shares it with. The GDPR requires organisations to maintain records of their processing activities.

It may therefore be necessary to organise **an information audit** (or a so-called data inventory) across the organisation. For example, if the organisation has inaccurate personal data and shared this with another organisation, it will have to tell the other organisation about the inaccuracy so it can correct its own records. This won't be possible unless the organisation knows what personal data it holds, where it came from and who it's shared with. This should be documented. Doing this will also help compliance with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

Step 3: Communicating privacy information

SAC should **review its current privacy notices** and put a plan in place for **making any necessary changes in time for GDPR implementation**. This is important for the organisation to ensure transparency.

When organisations collect personal data, they currently have to give people certain information, such as their identity and how they intend to use the personal information. This is usually done through a privacy notice.

Under the GDPR there are some **additional things organisations will have to tell people**. For example, they will need to **explain their lawful basis for processing the data**, their **data retention periods** and that the **individuals have a right to complain to the ICO** if they think there is a problem with the way the organisation is handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language.

In this regard, the SAC should consider **sending its members such a notice** as part of their GDPR compliance efforts. Please see https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/ in this regard for more detail.

Step 4: Individuals' (new) rights

The SAC should check its procedures to ensure it covers all the rights individuals have, including how it would delete personal data or provide data electronically and in a commonly used format. The nature of what the SACC does will mean that not all of the rights of individuals will be applicable to it.

The GDPR includes **the following rights for individuals**:

- the right to be informed (see Step 3 above);
- the right of access to a copy of the information comprised in their personal data;
- the right to rectification of incorrect personal data;
- the right to erasure or deletion of personal data (please note, it must be just as easy for the data subjects to withdraw their consent as it is for them to give consent);
- the right to restrict processing of personal data for the purpose of direct marketing (in many instances this would be similar to an opt-out option);
- the right to data portability (see below);
- the right to object to processing that is likely to cause or is causing damage or distress; and
- the right not to be subject to automated decision-making, including profiling.

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the Data Protection Act (DPA) but with some significant enhancements. If the organisation is geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check the organisation's procedures and to work out how it would react if someone asks to have their personal data deleted, for example. Would its systems help it to locate and delete the data? Who will make the decisions about deletion?

The right to data portability, which allows individuals to obtain and reuse their personal data for their own purposes across different services, is new. It only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

SAC should consider whether it needs to revise its procedures and make any changes. The organisation will need to provide the personal data in a structured commonly used and machine readable form and provide the information free of charge.

Step 5: Subject access requests

SAC should, if applicable, update its procedures and plan how it will handle access requests from Data Subjects, to take account of the new rules:

- In most cases the organisation will not be able to charge for complying with a request.
- The organisation will have a month to comply with such a request, rather than the current 40 days.
- The organisation can refuse or charge for requests that are manifestly unfounded or excessive.
- If a request is refused, the organisation must tell the individual why and that they have the right to complain to the supervisory authority (ICO) and to a judicial remedy. This must done without undue delay and at the latest, within one month.

If the organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. The organisation could for example consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online. **It might also be useful to have the SAC's Data Protection Policy, or the amended GDPR compliant policy, accessible to visitors on its website.**

Step 6: Lawful basis for processing personal data

The SACC should **identify the lawful basis for its processing activity in the GDPR**, document it and update its privacy notice to explain it.

Many organisations will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on the organisation's lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where the organisation uses consent as its lawful basis for processing.

The organisation will also have to explain its lawful basis for processing personal data in its privacy notice and when it answers a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the DPA. It should be possible to review the types of processing activities the organisation carries out and to identify its lawful basis for doing so. The organisation should document its lawful bases in order to help it comply with the GDPR's 'accountability' requirements.

Step 7: Consent

The SAC should **review how it seeks, records and manages consent and whether it needs to make any changes.** The SAC should **refresh the existing consent of members** now if they don't meet the GDPR standard.

The ICO has published detailed guidance on consent under the GDPR. This checklist (https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf) provides a useful tool to review the organisation's practices.

Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre- ticked boxes or inactivity. It must also be separate from other terms and conditions, and the organisation will need to have simple ways for people to withdraw consent. Consent has to be verifiable and individuals generally have more rights where the organisation relies on consent to process their data.

The organisation is not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But if it relies on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter these consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

Step 8: Children

In general, the SAC should start thinking now about whether it needs to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity. However, given the nature of what SAC does, it may not be necessary for it to be too concerned with this section.

For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If the organisation offers online services ('information society services') to children and relies on consent to collect information about them, then it may need a parent or guardian's consent in order to process their personal data lawfully. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger, then the organisation will need to get consent from a person holding 'parental responsibility'.

This could have significant implications if the organisation offers online services to children and collects their personal data. Remember that consent has to be verifiable and that when collecting children's data, the privacy notice must be written in language that children will understand.

Step 9: Data breaches

The SAC should make sure you **have the right procedures in place to detect, report and investigate a personal data breach**.

Some organisations are already required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. The organisation only has to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the organisation will also have to notify those concerned directly in most cases.

The organisation should put procedures in place to effectively detect, report and investigate a personal data breach. The organisation may wish to assess the types of personal data it holds and document where it would be required to notify the ICO or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

Step 10: Data protection by design and data protection impact assessment

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, **the GDPR makes privacy by design an express legal requirement,** under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and the organisation cannot sufficiently address those risks, the organisation will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

The organisation should therefore start to assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally?

The ICO has provided some very useful guidance on PIA's (https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf), which the SACC can consider to decide how to implement them in the organisation. This guidance shows how PIAs can link to other organisational processes such as risk management and project management.

The SAC can in any case adopt other more practical strategies for data protection. It should for example ensure the use of strong passwords on its electronic systems and the encryption of all portable devices for example.

Step 11: Data protection officers

The SAC should **designate someone to take responsibility for data protection compliance** and assess where this role will sit within the organisation's structure and governance arrangements. Such a person should receive sufficient training in this role if required.

The organisation should further consider whether it is required to formally designate a Data Protection Officer (DPO). The organisation must designate a DPO if it is:

- public authority (except for courts acting in their judicial capacity);
- an organisation that carries out the regular and systematic monitoring of individuals on a large scale; or
- an organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions.

It is most important that someone in the organisation, or an external data protection advisor, takes proper responsibility for the data protection compliance and has the knowledge, support and authority to carry out their role effectively.

Step 12: International

If the organisation operates in more than one EU member state, it should determine its lead data protection supervisory authority and document this.

The lead authority is the supervisory authority in the state where the organisation's main establishment is. The main establishment is the location where the organisation's central administration in the EU is or else the location where decisions about the purposes and means of processing are taken and implemented.

This is only relevant where the organisation carries out cross-border processing – i.e. it has establishments in more than one EU member state or it has a single establishment in the EU that carries out processing which substantially affects individuals in other EU states.

If this applies to the organisation, it should map out where it makes its most significant decisions about its processing activities. This will help to determine the 'main establishment' and therefore the lead supervisory authority.

Conclusion

As can be seen, there are a large number of issues to go through for GDPR compliance. However, there are some very useful tools for doing so. And it would be to the SAC's advantage to contact the ICO in terms of any issues it might have. The SAC is fortunately an organisation with limited scope in terms of the type of data it collects and what it uses this data for. Therefore, if the SAC already has a detailed data protection policy, it should not be a very complex process to ensure GDPR compliance.

[4] SA Congregations data protection policy

Evaluation-process

	Task	Relevant information – plan of action	Compliance
[1]	**Register with the ICO** - Information Commissioner's Office		**To do**
[2]	**<u>The GDPR legislation</u>** 1. Personal data shall be processed fairly and lawfully 2. Personal data shall be obtained only for one or more specific and lawful purposes 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. 4. Personal data shall be accurate and, kept up to date. 5. Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes. 6. Personal data shall be processed in accordance with the rights of data subjects under this Act. 7. Appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. 8. Personal data shall not be transferred to a country or territory outside the European Economic Area	**Full compliance** **Full compliance – data only used for relevant congregational activities** **Full compliance – only relevant data are processed** **Full compliance – yearly auditing of all data** **Full compliance – members free to unsubscribe, and such data is removed, but full checks will be run and data will be audited following new compliance guidelines** **See comments under 5** **Are working with Insight Support to ensure compliance** **Full compliance being investigated re making membership data available for churches in South Africa**	
	Allows employees, service users and other contacts to request to see the personal data held on them. This is	**Full compliance** - ***Members will have full right to access all their personal data***	

	called the **Data Access Request**		
[3]	**How to ensure compliance** **Step 1: Awareness** - employees informed about the upcoming changes. - risk register up to date - data protection refresher training for all staff **Step 2: Information the organisation holds** - Do an information audit: Document processing activities - what personal data do we hold, where it came from and who it shares it with. - **Step 3: Communicating privacy information** - **Review our current privacy notices** and **make any necessary changes required** - Note the following: **explain our lawful basis for processing the data**, the **data retention periods**, the **right to complain to the ICO** - **send members a notice** explaining these procedures **Step 4: Individuals' (new) rights** - The SAC should check its procedures to ensure it covers all the rights individuals have: The GDPR includes **the following rights for individuals**: • the right to be informed • the right of access to a copy of the information comprised in their personal data; • the right to rectification of incorrect personal data; • the right to erasure or deletion of personal data	**Proposed action: Meeting with all staff and employees** **Proposed action: organise an information audit** **Proposed action: Check procedures to comply with new legislation** **Proposed action: Check procedures to comply with new legislation**	**15 05 2018** **30 04 2018** **30 04 2018** **30 04 2018**

	• the right to restrict processing of personal data for the purpose of direct marketing • the right to data portability; • the right to object to processing that is likely to cause or is causing damage or distress; and • the right not to be subject to automated decision-making, including profiling. **Step 5: Subject access requests** SAC should, if applicable, update its procedures and plan how it will handle access requests from Data Subjects within a month **Is SAC's Data Protection Policy, or the amended GDPR compliant policy, accessible to visitors on its website?** **Step 6: Lawful basis for processing personal data** What is our **the lawful basis for its processing activity in the GDPR**, document it and update its privacy notice to explain it. **Step 7: Consent** The SAC should **review how it seeks, records and manages consent and whether it needs to make any changes.** The SAC should **refresh the existing consent of members** now if they don't meet the GDPR standard. **Step 8: Children**	**Proposed action: Check procedures to comply with new legislation** **Proposed action: Check procedures to comply with new legislation** **Proposed action: Check procedures to comply with new legislation**	**30 04 2018** **30 04 2018** **30 04 2018**

	In general, the SAC should start thinking now about whether it needs to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity. However, given the nature of what SAC does, it may not be necessary for it to be too concerned with this section.	**Full compliance**	
	Step 9: Data breaches		
	What **procedures do we have in place to detect, report and investigate a personal data breach**.	**Proposed action: Check procedures to comply with new legislation**	**30 04 2018**
	Step 10: Data protection by design and data protection impact assessment		
	Do we have **privacy by design in place as an express legal requirement,** under the term 'data protection by design and by default? How strong are our **passwords**?	**Proposed action: No DPIA process necessary at this stage , currently compliant, but will do check to ensure compliance**	**30 04 2018**
	Step 11: Data protection officers		
	Who is the designated person to take responsibility for data protection compliance?	**Proposed action: Check procedures to comply with new legislation**	**30 04 2018**
	Step 12: International		
	SAC operates only in die UK. What are the procedures for members that left the UK and are still subscribed to our database?	**Proposed action: Check procedures to comply with new legislation**	**30 04 2018**

Addendum: Data Protection Act 1998

Section 4(3).

SCHEDULE 2

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

1. The data subject has given his consent to the processing.
2. The processing is necessary—
    a. for the performance of a contract to which the data subject is a party, or
    b. for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary—
    a. for the administration of justice,

    [**F1**(aa)for the exercise of any functions of either House of Parliament,]

    b. for the exercise of any functions conferred on any person by or under any enactment,
    c. for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
    d. for the exercise of any other functions of a public nature exercised in the public interest by any person.

Annotations:

Amendments (Textual)

F1Sch. 2 para. 5(aa) inserted (1.1.2005) by 2000 c. 36, ss. 73, 87(3), Sch. 6 para. 4 (with ss. 56, 78); S.I. 2004/1909, **art. 2**; S.I. 2004/3122, **art. 2**

Modifications etc. (not altering text)

C1Sch. 2 para. 5 extended (2.12.1999) by S.I. 1999/3145, **arts. 1**, 9(3)(b); S.I. 1999/3208, **art. 2**

6. (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

    (2)The [**F2** Secretary of State] may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Annotations:

Amendments (Textual)

F2Words in Sch. 2 para. 6 substituted (19.8.2003) by The Secretary of State for Constitutional Affairs Order 2003 (S.I. 2003/1887), art. 9, **Sch. 2 para. 9(1)(b)**

Commencement Information

I1Sch. 2 para. 6 wholly in force at 1.3.2000; Sch. 2 para. 6 in force for certain purposes at Royal Assent see s. 75(2)(i); Sch. 2 para. 6 in force at 1.3.2000 insofar as not already in force by S.I. 2000/183, **art. 2(1)**

Amendments (Textual)

7. [**F3**The processing is necessary for the purposes of making a disclosure in good faith under a power conferred by—

a. section 21CA of the Terrorism Act 2000 (disclosures between certain entities within regulated sector in relation to suspicion of commission of terrorist financing offence or for purposes of identifying terrorist property), or

b. section 339ZB of the Proceeds of Crime Act 2002 (disclosures between certain entities within regulated sector in relation to money laundering suspicion).]

Annotations:

Amendments (Textual)

F3Sch. 2 para. 7 inserted (27.4.2017 for specified purposes, 31.10.2017 in so far as not already in force) by Criminal Finances Act 2017 (c. 22), s. 58(5)(6), **Sch. 5 para. 7**; S.I. 2017/991, reg. 2(m)

SCHEDULE 3

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE PERSONAL DATA

1. The data subject has given his explicit consent to the processing of the personal data.

2. (1)The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

   (2)The **[F1** Secretary of State**]** may by order—

   (a)exclude the application of sub-paragraph (1) in such cases as may be specified, or

   (b)provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

Annotations:

Amendments (Textual)

F1Words in Sch. 3 para. 2 substituted (19.8.2003) by The Secretary of State for Constitutional Affairs Order 2003 (S.I. 2003/1887), art. 9, **Sch. 2 para. 9(1)(b)**

Commencement Information

I1Sch. 3 para. 2 wholly in force at 1.3.2000; Sch. 3 para. 2 in force for certain purposes at Royal Assent see s. 75(2)(i); Sch. 3 para. 2 in force at 1.3.2000 insofar as not already in force by S.I. 2000/183, **art. 2(1)**

3. The processing is necessary—

   (a)in order to protect the vital interests of the data subject or another person, in a case where—

   (i)consent cannot be given by or on behalf of the data subject, or

   (ii)the data controller cannot reasonably be expected to obtain the consent of the data subject, or

   (b)in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing-

   (a)is carried out in the course of its legitimate activities by any body or association which—

   (i)is not established or conducted for profit, and

   (ii)exists for political, philosophical, religious or trade-union purposes,

   (b)is carried out with appropriate safeguards for the rights and freedoms of data subjects,

   (c)relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

   (d)does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing—

(a)is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b)is necessary for the purpose of obtaining legal advice, or

(c)is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7. (1)The processing is necessary—

(a)for the administration of justice,

[F2(aa)for the exercise of any functions of either House of Parliament,]

(b)for the exercise of any functions conferred on any person by or under an enactment, or

(c)for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2)The [F3 Secretary of State] may by order—

(a)exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b)provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

Annotations:

Amendments (Textual)

F2Sch. 3 para. 7(1)(aa) inserted (1.1.2005) by 2000 c. 36, ss. 73, 87(3), Sch. 6 para. 4 (with ss. 56, 78); S.I. 2004/1909, **art. 2**; S.I. 2004/3122, **art. 2**

F3Words in Sch. 3 para. 7 substituted (19.8.2003) by The Secretary of State for Constitutional Affairs Order 2003 (S.I. 2003/1887), art. 9, **Sch. 2 para. 9(1)(b)**

Modifications etc. (not altering text)

C1Sch. 3 para. 7 extended (2.12.1999) by S.I. 1999/3145, **arts. 1**, 9(3)(b); S.I. 1999/3208, **art. 2**

Commencement Information

I2Sch. 3 para. 7 wholly in force at 1.3.2000; Sch. 3 para. 7 in force for certain purposes at Royal Assent see s. 75(2)(i); Sch. 3 para. 7 in force at 1.3.2000 insofar as not already in force by S.I. 2000/183, **art. 2(1)**

[F47A(1)The processing—

(a)is either—

(i)the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or

(ii)any other processing by that person or another person of sensitive personal data so disclosed; and

(b)is necessary for the purposes of preventing fraud or a particular kind of fraud.

(2)In this paragraph "an anti-fraud organisation" means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes.]

Annotations:

Amendments (Textual)

F4Sch. 3 para. 7A inserted (1.10.2008) by Serious Crime Act 2007 (c. 27), **ss. 72**, 94; S.I. 2008/2504, **art. 2(e)**

[F57BThe processing is necessary for the purposes of making a disclosure in good faith under a power conferred by—

(a)section 21CA of the Terrorism Act 2000 (disclosures between certain entities within regulated sector in relation to suspicion of commission of terrorist financing offence or for purposes of identifying terrorist property), or

(b)section 339ZB of the Proceeds of Crime Act 2002 (disclosures within regulated sector in relation to money laundering suspicion).]

Annotations:

Amendments (Textual)

F5Sch. 3 para. 7B inserted (27.4.2017 for specified purposes, 31.10.2017 in so far as not already in force) by Criminal Finances Act 2017 (c. 22), s. 58(5)(6), **Sch. 5 para. 8**; S.I. 2017/991, reg. 2(m)

8. (1)The processing is necessary for medical purposes and is undertaken by—

(a)a health professional, or

(b)a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2)In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. (1)The processing—

(a)is of sensitive personal data consisting of information as to racial or ethnic origin,

(b)is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(c)is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2)The [F6 Secretary of State] may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

Annotations:

Amendments (Textual)

F6Words in Sch. 3 para. 9 substituted (19.8.2003) by The Secretary of State for Constitutional Affairs Order 2003 (S.I. 2003/1887), art. 9, **Sch. 2 para. 9(1)(b)**

Commencement Information

I3Sch. 3 para. 9 wholly in force at 1.3.2000; Sch. 3 para. 9 in force for certain purposes at Royal Assent see s. 75(2)(i); Sch. 3 para. 9 in force at 1.3.2000 insofar as not already in force by S.I. 2000/183, **art. 2(1)**

10The personal data are processed in circumstances specified in an order made by the **[F7** Secretary of State**]** for the purposes of this paragraph.

Annotations:

Amendments (Textual)

F7Words in Sch. 3 para. 10 substituted (19.8.2003) by The Secretary of State for Constitutional Affairs Order 2003 (S.I. 2003/1887), art. 9, **Sch. 2 para. 9(1)(b)**

Commencement Information

I4Sch. 3 para. 10 wholly in force at 1.3.2000; Sch. 3 para. 10 in force for certain purposes at Royal Assent see s. 75(2)(i); Sch. 3 para. 10 in force at 1.3.2000 insofar as not already in force by S.I. 2000/183, **art. 2(1)**

[5] Implikasies en vrae vir SAG:

Uitdaging om datalyste anders te hanteer – moet kan verduidelik waarom ons watter inligting van lidmate nodig het en gebruik

- Huidige lidmate op databasis
    - **A lidmate** moet "OPT-IN" en ons moet as bewys hiervan hul reaksie bewaar – maw 'n tipe van consent form, geen reaksie = 'n nee antwoord en mag ons nie hul data hou en gebruik nie
    - **B lidmate** – mag heel waarskynlik net naam en e-poste hou – maar hulle moet ook toestemming daarvoor gee, maw dus ook "OPT-IN"
    - **Formers** almal delete – ons mag nie data hou nie

        Om te doen: *sal 'n e-pos opstel wat aan lidmate proses verduidelik en opsies uiteensit dalk opsie om nuut te begin met alle data...*

- **Ons mag geen datalyste (van enige aktiwiteit) hou nie**
    - Verwerk en delete so gou as moontlik na event ook op persoonlike rekenaars
    - Bcc groepe in e-poste
    - Intekenlyste nuut dink – ondersoek elektroniese opsies, dalk net name en nie kontak-inligting
    - Bedieningslyste en roosters – moet ook toestemming van lidmate daarvoor hê, werk dalk net met name en nie ook telno en e-pos adresse nie...
    - Geld ook vir wattsapp groepe

- Op en tydens **lewendige uitsendings** moet kennisgewings oor data-beskerming duidelik vertoon word

- **Opleiding** vir personeel, opleidings- en inligtings-proses volg lidmate

- **Bewyse van lidmaatskap**: beste opsie lyk of ons direk vir lidmate wat die gemeente verlaat bewys van lidmaatskap saamgee, aangesien ons nie data mag hou van mense wat die gemeente verlaat nie. Dit moet ook verduidelik word aan huidige lidmate. *Moet dit nog uitklaar*

- Toestemming vir gebruik van **fotos**

- **Ander policies** moet aangepas word en duideliik sigbaar en beskikbaar wees op web

[6] Voorgestelde mail aan gemeente

Die Data Protection wet (GDRP)in die VK verander en as gemeente moet ons seker maak dat ons julle data reg hanteer, binne die raamwerk van die wet. Dit bied ons ook ‘n uitstekende geleentheid om ons data op datum te kry.
Die nuwe wet vereis ook dat jy ons as direk toestemming moet gee om jou besonderhede te hê en te gebruik, so jy moet asseblief op hierdie e-pos reageer.

Dit gaan jou nie langer as 5 min neem nie, maar help ons asseblief!!
Kliek in die boksie van toepassing en volg die aanwysings:

□ Ek is nie meer ‘n lidmaat van SA Gemeente nie en wil nie meer korrespondensie ontvang nie. Reply asseblief op hierdie e-pos met die woord “Unsubscribe”. Ons verwyder jou data dan van ons databasis af.

□ Ek is nie meer ‘n lidmaat van SA Gemeente nie, maar wil nog korrespondensie van die gemeente ontvang. Bevestig hier jou e-pos adres, waarmee jy vir ons toestemming gee om net jou e-pos adres op ons databasis te hou. Alle ander data sal verwyder word.

□ Ek is steeds ‘n lidmaat van SA Gemeente en gee toestemming dat ek gekontak mag word én die gemeente my data mag gebruik vir gemeente sake.

As jy die laaste blokkie gekies het, volg assbelief die hierdie skakel om jou data te bevestig.

- Kliek op "Log in|Register" regs bo op die webbladsy.
- Jou "login name" en "password" vir SA Gemeente is:
  Login name: {naam.van}
  Password: { password}

  Doen dan die volgende:
  - Verander jou "password" na iets wat jy makliker kan onthou. Om dit te doen, kliek op "My Area" en volg dan My Area > My Details > Change Password

  - Gaan kyk ook asb of jou inligting korrek en volledig is deur in te log (soos hierbo) en na "My Area" te navigeer. Jy kan ook jou gesin se besonderhede so opdateer. Maak asb seker dat die inligting so volledig as moontlik is. Geboorte datums, huwelikstatus, email, adres en telefoon nommers.

  - Voeg enige gesinslede (man, vrou en/of kinders) by jou rekord sodat ons van hulle weet. Ons verwys veral na al die nuwe pasgebore lidmate van ons gemeente. Kliek weereens op "My Area". Kliek op "Add to Family" en volg die instruksies.

Kontak ons gerus by info@sagemeente.com as enige iets onduidelik is of vir enige verder inligting of navrae oor die gemeente.